UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,873	11/22/2005	Marc Joye	032326-301	6724

21839 7590 01/25/2010
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
01/25/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	**Application No.** 10/534,873	**Applicant(s)** JOYE ET AL.
	Examiner BRYAN WRIGHT	**Art Unit** 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/23/2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 10/23/2009. Claims 1, 3, 4, 6, 10 and 11 have been amended. Claims 1-13 are pending.

Claim Objections

2. Claims 3, 6, 10, and 11 are objected to because of the following informalities: The applicant is advised of Rule 1.96 of the MPEP, for which states a computer program listing of 300 lines or less may be submitted in a drawing or part of the specification. See MPEP Rule 1.96. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 3, 6, 10, and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 3, 6, 10, and 11 cannot be construed by one of ordinary skill in the art to distinctly point out definitive claim limitations. The subject matter in claims 3, 6, 10, and 11 merely describes “programmatic" steps that one of ordinary skill in the art would use in rendering the necessary program execution in accordance with the claimed invention. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes (NPL "Handbook of applied cryptography" (cited from IDS)) in view of Drexler et al. (US 2003/0061498 and Drexler hereinafter)

5. As to claim 1, Menezes teaches a cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device (i.e., ...teaches integer division [pg. 63, sect. 2.79]), with where q is a quotient [pg. 64, sect. 2.82], a is a number of containing m bits [pg. 64, sect. 2.82], b is a number of containing n bits [pg. 64, sect. 2.82], with n less than or equal to m and b.-, is non-zero, bnq being the most significant bit of b [pg. 64, sect. 2.83],

a comprising the following steps: (i) performing a partial division of a word A, comprising left n bits of the number a. by the number b to obtain a bit of the quotient q, (i.e., ...teaches integer division [pg. 63, sect. 2.79]);

Menezes does not expressly teach: (ii) repeating step (i) for m-n + 1 iterations (e.g., For Loop) with the same number and type operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q.

However, Menezes discloses instruction for which could be implemented as a "Computer For Loop Condition Statement" for iterative calculation of the encryption process as recited on [pg. 598, sect. 14.20].

Therefore given applicants minor change of the "For Loop" instruction to be iterated through (e.g., carryout by the computer) the encryption process, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Meneze's "For Loop Condition Statement" by employing the well known feature of adding an additional iterative step (e.g.., (n+l)) for which will enhance data encryption within a chip card [pg. 598, sect. 14.20].

Menezes does not expressly teach:
wherein at least one of the numbers a and b comprises secret data and (iii) generating encrypted or decrypted data in accordance with said quotient.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Menezes as introduced by Drexler. Drexler discloses: wherein at least one of the numbers a and b comprises secret data (to provide use of a secret key (e.g., secret data) in the calculation [par. 18]) and (iii) generating encrypted or decrypted data in accordance with said quotient (to provide a procedure for encrypting text with the use of a quotient [par. 23; fig. 1].

Therefore, given the teachings of Drexler, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Menezes by employing the well known feature of encrypting text using a quotient produced in integer division disclosed above by Drexler, for enhancing encryption in a chip card. [fig. 1].

6. As to claim 2, Menezes a method where at each iteration, an addition of the number b to the word A and a subtraction of the number b from the word A are performed [pg. 598, sect. 14.20, 3.1].

7. As to claim 3, Menezes a method where all the following steps are performed: Input a = (0, am-,, ..., a0) b = (bn-1, ..., bo) [pg. 598, sect. 14.20], Output: q = a div b and r = a mod b [pg. 598, sect. 14.20]. Menezes does not expressly teach: A = (0, am-l-], ..., am-n+0 ;o' - 1 For j = 1 to (m-n+ 1), do: a - SHLm+ll(a, 1) ; o' - carry A - (c')SUB,(A, b) + (-')ADD,(A, b) o- -(o' AND -') / (o' AND carry)/(o' AND carry) lsb(a) g'-'-(3' End For if (-o = TRUE) then A - ADDn,(A, b), wherein the symbol - indicates loading of a content of a register containing data on the right of the symbol in a register whose data has the label on the left of the symbol; wherein a indicates whether or not a subtraction has

been performed wrongly; wherein o' is a negation of o; wherein o' is a variable to preserve the value of o,obtained in a previous iteration; wherein TRUE is a constant; wherein lsb(a) is the lowest weight bit of the number a; wherein $SHL_{m+l}(a, 1)$ is an operation of shifting to the left by 1 bit in the register of m+1 bits containing the data item a, the bit leaving the register being stored in the variable carry and a bit equal to 0 being entered as the least significant bit of the register initially containing the data a; wherein $ADD_n(A, b)$ is an operation of addition of the n bits of the number b to the n bits of the word A; and wherein $SUB_n(A, b)$ is an operation of subtraction of the number b from the word A. However, Menezes discloses instruction for performing encryption utilizing integer division which could be implemented in the form of a "Computer For Loop Condition Statement". Menezes' iterative calculation of the encryption process is recited on [pg. 598, sect. 14.20]. Therefore given applicants minor change of the "For Loop" instruction to be iterated through (e.g., carryout by the computer) the encryption process, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Meneze's "For Loop Condition Statement" by employing the well known feature of adding an additional iterative step (e.g.., (n+l)) for which will enhance data encryption within a chip card [pg. 598, sect. 14.20].

8. As to claim 4, Menezes teaches a method where at each iteration (e.g., "For Loop Iteration"), either the number b or of a number complementary to the number b is added to the word A [pg. 598, sect. 14.20].

9. As to claim 5, Menezes teaches a method further at each iteration, an of updating of a first variable (c') (e.g., "x") indicating whether, during the following iteration, the number b or the number b must is to be added with the word A according to the quotient bit produced. [pg. 598, sect. 14.20].

As to claim 6, Menezes teaches a method where all the following steps are performed: Input: a = (0, am-,, ..., a0) b = (b,-,, ..., bo) [pg. 598, sect. 14.20], and Output: q = a div b and r = a mod b [pg. 598, sect. 14.20]. Menezes does not expressly teach: A = (0, am-I-], ..., arc-I-;o' - 1; b -CPL2n(b) Forj = 1 to (m-n+ 1), do: a - SHLm+II(a, 1) ; o' - carry daddr -A - baddr + o'(b' - baddr) (c')SUB,(A, b) + (-')ADD,(A, b) c- -(-' AND -') / (c' AND carry)/(c' AND carry) Isb(a) g' -' -(3' End For if (~ = TRUE) then A- ADD,(A, b), wherein the symbol <- indicates loading of a content of a register containing data on the right of the symbol in a register containing data on the left of the symbol; wherein ~ indicates whether or not a subtraction has been performed wrongly; wherein -~a is a negation of c; wherein a' is a variable to preserve the value of ~ obtained in a previous iteration; wherein TRUE is a constant; wherein Isb(a) is the lowest weight bit of the number a;wherein SHL_{m+1}(a, 1) is an operation of shifting to the left by 1 bit in the register of m+l bits containing the data item a, the bit leaving the register being stored in the variable carry and a bit equal to 0 being entered as the least significant bit of the register initially containing the data a; wherein ADD_n(A, b) is an operation of addition of the n bits of the number b to the n bits of the word A; wherein addr denotes address of a variable; and wherein complement to 2^n of a number is obtained by the $CPL2_N$ of the number. However, Menezes discloses instruction for performing encryption utilizing integer division which could be implemented as a "Computer For Loop Condition Statement" Menezes' iterative calculation of the encryption process is recited on [pg. 598, sect. 14.20]. Therefore given applicants minor change of the "For Loop" instruction to be iterated through (e.g., carryout by the computer) the encryption process, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Meneze's "For Loop Condition Statement" by employing the well known feature of adding an additional iterative step (e.g.., (n+l)) for which will enhance data encryption within a chip card [pg. 598, sect. 14.20].

10. As to claim 7, Menezes teaches a method during which further including the steps, at each iteration, of performing an operation of complement to 2n of an updated data item (b or b) or of a notional data item (c or c) and then-an adding the updated data item with the word A (pg. 598, 14.20, lines 2 and 3).

11. As to claim 8, Menezes teaches a method, further including the step, at each iteration, of updating a second variable (e.g., "n") is-also indicating whether, during the following iteration, the operation of complement to 2n must is to be performed on the updated data item or on the notional data item. (pg. 598, 14.20, lines 2 and 3).

12. As to claim 9, Menezes teaches a method further including the step, at each iteration, of updating of a third variable (e.g., "x") indicating whether the updated data item is equal to the data item b or to its complement to 2n (pg. 598, sect. 14.20).

13. As to claim 10, Menezes teaches a method according to one-of which claim 7, wherein all the following steps are also performed: Input a = (0, am4, ..., a0) b = (bn-1, ..., b0) [pg. 598, sect. 14.20], and Output: q = a div b and r = a mod b [pg. 598, sect. 14.20]. Menezes does not expressly teach: o' - 1 ; B - 1, y - 1 ; A = (0, am-, ... , am--n+1) for j = 1 to (m-n+ 1), do: a -SHLm÷x(a, 1);a -carry 8 -o'113 daddr - baddr + 8 (Caddr -- baddr) d - CPL2.(d) A - ADDn(A, b) o -(o AND o') / (cr AND carry)/(or' AND carry) B -o';y-y/8;o' -o Isb(a) = o' end for if (-Io = TRUE) then A - ADD,(A, b), wherein the symbol <- indicates loading of a content of a register containing data on the right of the symbol in a register containing data on the left of the symbol; wherein (~ indicates whether or not a subtraction has been performed wroingly; wherein –o' is a negation of o'; wherein o' is a variable to preserve the value of o' obtained in a previous iteration; wherein TRUE is a constant; wherein Isb(a) is the lowest weight bit of the number a; wherein SHL$_{m+1}$l(a, 1) is an operation of shifting to the left by 1 bit in the register of m+l bits containing the data item a, the bit leaving the register being stored in the variable carry and a bit equal to 0 being entered as the least significant bit of the register initially containing the data a; wherein ADD$_n$(A, b) is an operation of addition of the n bits of the number b to the n bits of the word A; wherein addr denotes address of a variable; and wherein 13 and 7 are variables. However, Menezes discloses instruction for performing

encryption utilizing integer division which could be implemented as a "Computer For Loop Condition Statement". Menezes' iterative calculation of the encryption process is recited on [pg. 598, sect. 14.20]. Therefore given applicants "For Loop" instruction to be iterated through (e.g., carryout by the computer) the encryption process, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Meneze's "For Loop Condition Statement" by employing the well known feature of adding an additional iterative step (e.g.., (n+l)) for which will enhance data encryption within a chip card [pg. 598, sect. 14.20].

14. As to claim 11, Menezes teaches a method where at the end, the following operations are performed : if (713 = TRUE) then b - CPL2n(b) if (-y = TRUE) then o' CPL2,(o')., wherein -~B is a negation of B; and wherein ~y is a negation of y (i.e., ... teaches condition if...then.., statement logic [pg. 598, sect. 14.20, line 3.1]).

15. As to claims 12 and 13, although the teaching of Menezes discloses substantial features of the claim invention it does not disclose: An electronic component comprising calculation means programmed to implement a method said calculation means comprising a central unit associated with a memory comprising several registers for storing the data a and b (claim 12).

A chip card comprising an electronic component according to Claim 12. (claim 13).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Menezes as introduced by Drexler. Drexler discloses:

An electronic component comprising calculation means programmed to implement a method said calculation means comprising a central unit associated with a memory comprising several registers for storing the data a and b (claim 12) (to provide encryption processing means using integer division on a chip card [abstract]).

A chip card comprising an electronic component according to claim 12, (claim 13). (to provide encryption processing means using integer division on a chip card [abstract]).

Therefore, given the teachings of Drexler, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Menezes by employing the well known feature of chip card data encryption disclosed above by Drexler, for enhancing chip card security [abstract].

Response to Arguments

Remarks - 101 Rejection

The Examiner withdraws rejection made under 101 for claim 1 in view of applicant's amendment.

Remarks – 112th 2nd Paragraph Rejection – Claims 3, 6, 10,and 11

The Examiner maintains rejection made under 112th 2nd Paragraph for claims 3, 6, 10 and 11. The Examiner contends the claimed subject matter of these claims are based on program procedural steps and therefore do not clearly define the metes and bounds of the claim.

Remarks – 103 Rejection - Claims 1-13

With regard to applicant's remarks of, 'Menezes does not disclose an integer division method with the same operations being performed at each iteration of obtaining a bit of the quotient, as described in claim 1", the Examiner contends Menezes discloses the use of a "For Loop" to carryout an integer division operation. Those skilled in the art would recognize the iterative nature of a "For Loop" and that such a loop is used to precisely carryout a desired operation. In this instance said desire operation is performing integer division.

With regard to applicant's remarks of, "according to the method in Menezes, the operations performed at one iteration might be different from another iteration", the

Examiner contends in this instance the term "different" is used in accordance with loop output value and the action iterative process. Those skilled in the art would recognize while the output value will change, the way in which the iterative integer division process is carried out will not change until the condition of the “For Loop” is met.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431